



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/010,031	11/30/2001	Michael F. Angelo	1662-39900 JMH (P00-3100)	4706
22879	7590	10/03/2005	EXAMINER	
HEWLETT PACKARD COMPANY P O BOX 272400, 3404 E. HARMONY ROAD INTELLECTUAL PROPERTY ADMINISTRATION FORT COLLINS, CO 80527-2400			LASHLEY, LAUREL L	
			ART UNIT	PAPER NUMBER
			2132	

DATE MAILED: 10/03/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	10/010,031	ANGELO ET AL.	
	Examiner	Art Unit	
	Laurel Lashley	2132	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) Responsive to communication(s) filed on 30 November 2001.
- 2a) This action is FINAL. 2b) This action is non-final.
- 3) Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) Claim(s) 1-35 is/are pending in the application.
- 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) Claim(s) _____ is/are allowed.
- 6) Claim(s) 1-35 is/are rejected.
- 7) Claim(s) _____ is/are objected to.
- 8) Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) The specification is objected to by the Examiner.
- 10) The drawing(s) filed on 30 November 2001 is/are: a) accepted or b) objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
 - a) All
 - b) Some *
 - c) None of:
 1. Certified copies of the priority documents have been received.
 2. Certified copies of the priority documents have been received in Application No. _____.
 3. Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).
- * See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- | | |
|---|---|
| 1) <input checked="" type="checkbox"/> Notice of References Cited (PTO-892) | 4) <input type="checkbox"/> Interview Summary (PTO-413) |
| 2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948) | Paper No(s)/Mail Date. _____ |
| 3) <input checked="" type="checkbox"/> Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
Paper No(s)/Mail Date _____ | 5) <input type="checkbox"/> Notice of Informal Patent Application (PTO-152) |
| | 6) <input type="checkbox"/> Other: _____ |

DETAILED ACTION

1. Claims 1-35 have been examined.

Information Disclosure Statement

2. The information disclosure statement (IDS) submitted on 26 February 2002 was filed after the mailing date of the application on 30 November 2001. The submission is in compliance with the provisions of 37 CFR 1.97. Accordingly, the information disclosure statement is being considered by the examiner.

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

3. Claims 1 – 22 are rejected under 35 U.S.C. 102(b) as being anticipated by Sudia in US Patent 5, 659,616 (hereinafter US '616).

As it pertains to claim 1, US '616 teaches:

A method of establishing a secured communication session across a remote network connection, comprising (see Figure 5):

- (a) receiving a first certificate (see column 9, line 38; basic key certificate) that includes a first digital signature (see column 9, line 39 and Figure 5, item 55; sender's signature);
- (b) obtaining a first public key (See Figure 5; where it is inherent that the public key is included in the certificate has been sent);
- (c) using the first public key to verify the first digital signature (see column 9, line 39);

- (d) if the first digital signature in (c) is successfully verified, receiving a second certificate that includes a second digital signature (see column 9, lines 54 – 55;);
- (e) obtaining a second public key (see column 9, line 61; sponsor's public key); and
- (f) using the second public key to verify the second digital signature (see column 9, line 60; sponsor's signature).

For claim 2, US '616 teaches:

The method of claim 1 wherein said first and second digital signatures are signed with different private keys (see column 16, lines 66 – 67 and column 17, lines 1 – 5; where it is inherent that if private keys are self-confined then they must be different).

For claim 3, US '616 teaches:

The method of claim 1 wherein said second certificate includes at least a portion of said first certificate (see column 9, line 43; where it is inherent that if authorization certificated is appended to the basic key certificate then it must be at least a portion of the certificate).

For claim 4, US '616 teaches:

The method of claim 1 wherein (c) includes decrypting a portion of said first certificate to recover a first hash value (see column 12, lines 37 – 40).

For claim 5, US '616 teaches:

The method of claim 4 wherein (c) also includes computing a hash of at least a portion of said first certificate to produce a first computed hash value (see column 12, lines 40 – 44).

For claim 6, US '616 teaches:

Art Unit: 2132

The method of claim 5 wherein said first hash value is compared to said first computed hash value (see column 11, lines 31 – 34; where the hash matches).

For claim 7, US '616 teaches:

The method of claim 6 wherein (c) further includes determining said first digital signature is successfully verified if said first hash value matches said first computed hash value (column 12, lines 16 – 18 where successful matches for counterparty values is achieved successfully).

For claim 8, US '616 teaches:

The method of claim 1 wherein (f) includes decrypting a portion of said second certificate to recover a second hash value (see column 12, lines 37 – 40).

For claim 9, US '616 teaches:

The method of claim 8 wherein (f) also includes computing a hash of at least a portion of said second certificate to produce a second computed hash value (see column 12, lines 40 – 44).

For claim 10, US '616 teaches:

The method of claim 9 wherein said second hash value is compared to said second computed hash value (see column 11, lines 31 – 34).

For claim 11, US '616 teaches:

The method of claim 10 further including successfully verifying said second digital signature if said second hash value matches said second computed hash value (see column 12, lines 16 – 18).

As it relates to claim 12, US '616 teaches:

Art Unit: 2132

A method of establishing a secured communication session across a remote network connection, comprising:

- (a) receiving first and second certificates that include first and second digital signatures, respectively (see column 9, lines 39 and 54 - 55);
- (b) obtaining first and second public keys (see Figure 5 and column 9, line 61);
- (c) using the first public key to verify the first digital signature (see column 9, lines 39 and 61);
- (d) if the first digital signature in (c) is successfully verified, verifying the second digital signature; and (e) permitting the communication session to occur if both said first and said second digital signatures are successfully verified (see column 9, lines 54 - 55 and 60).

For claim 13, US '616 teaches:

The method of claim 12 wherein said first and second digital signatures are signed with different private keys (see column 16, lines 66 – 67 and column 17, lines 1 – 5).

For claim 14, US '616 teaches:

The method of claim 12 wherein said second certificate includes at least a portion of said first certificate (see column 9, line 43).

For claim 15, US '616 teaches:

The method of claim 12 wherein (c) includes using said first public key to decrypt a portion of said first certificate to recover a first hash value (see column 2, line 64).

For claim 16, US '616 teaches:

The method of claim 15 wherein (c) also includes computing a hash of at least a portion of said first certificate to produce a first computed hash value (see column 12, lines 40 – 44).

For claim 17, US '616 teaches:

The method of claim 16 wherein (c) includes comparing said first hash value to said first computed hash value (see column 11, lines 31 – 34).

For claim 18, US '616 teaches:

The method of claim 17 wherein (c) further includes determining that said first digital signature is successfully verified if said first hash value matches said first computed hash value (see column 12, lines 16 – 18).

For claim 19, US '616 teaches:

The method of claim 12 wherein (c) includes decrypting a portion of said second certificate to recover a second hash value (see column 12, lines 37 – 40).

For claim 20, US '616 teaches:

The method of claim 19 wherein (c) also includes computing a hash of at least a portion of said second certificate to produce a second computed hash value (see column 12, lines 40 – 44).

For claim 21, US '616 teaches:

The method of claim 20 wherein (c) includes comparing said second hash value to said second computed hash value (see column 11, lines 31 – 34).

For claim 22, US '616 teaches:

The method of claim 21 further including successfully verifying said second digital signature if said second hash value matches said second computed hash value (see column 12, lines 16 – 18).

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

4. Claims 23 – 25 are rejected under 35 U.S.C. 102(e) as being anticipated by Tycksen, Jr. et al. in US Patent 6,189,097 B1 (hereinafter US '097).

As it relates to claim 23, US '097 teaches:

A method of creating a remotely verifiable certificate (see column 3, line 38), comprising:

- (a) retrieving a first signed certificate (see column 4, line 12 and Figures 1 and 7);
- (b) combining together said first signed certificate with other values (see Figures 1 and 3);
- (c) computing a hash of the combination from (b) (see column 5, lines 52 – 53); and
- (d) signing said hash from (c) with a private key (see Figure 7 and column 9, lines 35 – 52).

For claim 24, US '097 teaches:

Art Unit: 2132

The method of claim 23 wherein said other values in (b) includes an IP address (see column 13, lines 22 – 23; where a digital certificate can carry a number of components; and see column 6, lines 65 – 66; where it is inherent that if a digital certificate can be stored on a personal computer (PC) it will contain that PC's IP address).

For claim 25, US '097 teaches:

The method of claim 23 wherein said other values in (b) includes a domain name (see column 13, lines 22 – 24 and column 6, line 47; where a website component is equivalent to a domain name).

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

5. Claims 26 and 32 – 35 are rejected under 35 U.S.C. 102(b) as being anticipated by Van Oorschot in US Patent 6,134,327 (hereinafter '327).

Art Unit: 2132

As it pertains to claim 26, US '327 teaches:

A computer, comprising:

a processor (see column 9, line 46); and

a memory coupled to said processor (see column 9, line 47);

wherein said memory includes storage for a first certificate and a second certificate,

said second certificate derived from said first certificate (see column 9, lines 66 – 67

and column 10; lines 3 – 4).

As it relates to claim 32, US '327 teaches:

A client system, comprising:

a processor (see column 9, line 46); and

a memory coupled to said processor (see column 9, line 47); and

a connection to a communication link to a server (see Abstract; communication system);

wherein said processor requests a first certificate from the server, verifies a first digital

signature associated with said first certificate, and if said first digital signature is

successfully verified, requests a second certificate from said server and verifies a

second digital signature associated with said second certificate (see Figure 5 and

column 8, lines 18 – 45).

For claim 33, US '327 teaches:

The client system of claim 32 wherein the client uses two different public keys to verify

the first and second digital signatures (see column 10, line 24; where the public key of

the associated public key was used to authenticate said certificated and where it is

inherent that the public key certificate would use its own key).

As for claim 34, US '327 teaches:

A client system, comprising:

a processor (see column 9, line 46);

a memory coupled to said processor (see column 9, line 47); and

a connection to a communication link to a server (see Abstract; communication system);

wherein said processor requests a first certificate and a second certificate from the

server, verifies a first digital signature associated with said first certificate, and if said

first digital signature is successfully verified, verifies a second digital signature

associated with said second certificate (see Figure 5 and column 8, lines 18 – 45).

For claim 35, US '327 teaches:

The client system of claim 34 wherein the client uses two different public keys to verify the first and second digital signatures (see column 10, line 24).

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

6. Claims 27 – 31 are rejected under 35 U.S.C. 103(a) as being unpatentable over Van Oorschot in US '327 as applied to claim 26 above, and further in view of Tycksen, Jr. et al. in US '097.

For claim 27, US '327 shows a computer system but does not teach wherein said processor combines at least a portion of said first certificate with additional values, computes a hash of said combination, and encrypts said hash with a private key as taught by US '097 (see column 9, lines 39 – 40; where it is inherent that the combination will be hashed using a private key (hash also known as a message digest)).

For claim 28, US '327 shows a computer system but does not teach wherein said additional values include an IP address as taught by US '097 (see column 13, lines 22 – 23 and column 6, lines 65 – 66).

For claim 29, US '327 shows a computer system but does not teach wherein said additional values include a domain name as taught by US '097 (see column 13, lines 22 – 24 and column 6, line 47).

For claim 30, US '327 shows a computer system but does not teach wherein said first certificate includes a serial number as taught by US '097 (see Figure 1, item 11a).

For claim 31, US '327 shows a computer system but does not teach wherein said first certificate is not created by the server as taught by US '097 (see Figure 3, item 102 and column 7, lines 59 – 62).

For claims 27 – 31, it would be obvious to one of ordinary skill in the art at the time of the invention to modify Van Oorschot's method to Tycksen, Jr. et al.'s for the purpose of utilizing the certificate's functionality of secure communication while retaining identifying components to verify its origin and validity.

Art Unit: 2132

Conclusion

7. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure. US 5,373,561 as anticipated by Haber et al. discloses a new certificated which is derived from an original certificate. US 6,249,873 B1 as anticipated by Richard et al. discloses ideas parallel to applicant's claimed invention.

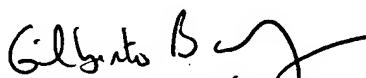
Any inquiry concerning this communication or earlier communications from the examiner should be directed to Laurel Lashley whose telephone number is 571-272-0693. The examiner can normally be reached on 7:30 am - 5 pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gilberto Barron, Jr. can be reached on 571-272-3799. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Laurel Lashley
Examiner
Art Unit 2132

September 26, 2005


GILBERTO BARRON
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100